



PAYMENTS INSIDER

The inside scoop on payments for businesses of all sizes

INSIDE: Why You Need the <i>ACH Rules</i>	pg. 1
New Return Code Alerts Companies to Fraud.....	pg. 1
Securing Data at Your Company.....	pg. 2
Mitigating Check Fraud at Your Business.....	pg. 3
Ho-Ho-How to Reduce Card Fraud this Holiday Season.....	pg. 4
OFAC Compliance Facts Every Business Should Know	pg. 5

Alexa, Can You Read This Article on Voice Assistants?	pg. 6
Busting Payments Myths.....	pg. 7
Federal Reserve to Launch FedNow SM	pg. 7
Why it Pays for Nonprofits to Encourage ACH/EFT Donations.....	pg. 8
White Paper Examines the Effects of Synthetic Identity Payments Fraud.....	pg. 9

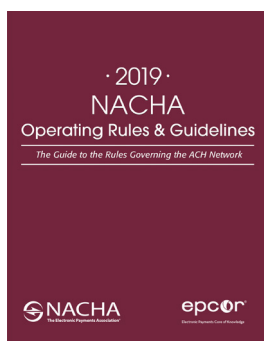
Why You Need the ACH Rules

by Jen Kirk, AAP, Vice President, Education

Why should you, the corporate user, care what the *ACH Rules* say? Because your agreement with your financial institution legally binds you to the *ACH Rules*!

Generally speaking, the *ACH Rules* is written for financial institutions. However, the legally binding contract you and your financial institution (ODFI) have with one another most likely states that all rights, responsibilities and warranties are transferred to you. Look at the contract your business signed with your financial institution that handles your ACH transactions (it is probably called an ODFI/Originator Agreement). If the words, “Company agrees to comply with and be bound by the *Rules*,” appear in your contract then you are indeed now tied to the *ACH Rules*. And, in essence, this means that you are required to follow any rule that says “ODFI” in the wording.

Here are five ways you can access the *ACH Rules* or applicable payments changes:



1. Preorder EPCOR's [ACH Quick Reference Guide for Corporate Users](#).
2. *Payments Insider*. The publication you are reading right now is a great tool to keep you up-to-date on recent payments-related issues! Here's a [link](#) to the article we run each Spring for rules changes that are important to companies.
3. [ACH Quick Reference Cards for Corporate Users](#). This three-card series gives companies fingertip access to critical information for the correct handling of ACH Returns, Dishonored Returns, Standard Entry Class (SEC) codes, Transaction codes and Notifications of Change (NOC).
4. Purchase a hard copy, electronic access or app version of the [ACH Rules](#). The easiest way to stay compliant is to have the rules in hand! Order your copy of the 2019 *ACH Rules* today!
5. Become an EPCOR member. Becoming an EPCOR member gives you access to many resources to help you maintain compliance with the various payment systems rules and regulations. If you're interested in becoming a member, reach out to Member Support at 800.500.0100 or via email at memserve@epcor.org.

New Return Code Alerts Companies to Fraud

by Shelly Sipple, AAP, APRP, NCP, Director, Certifications & Continuing Education

You send transactions out into the ACH Network under the assumption the account number is correct. But, what happens when the account number is wrong or invalid?

A financial institution who receives an ACH payment initiated by your company may post it based solely on the account number information you provided in the entry. And, if they can't post it that way, they may:

1. Manually post it to the recipient's account and send a Notification of Change (NOC) with the corrected account information to your company, or
2. They may return the payment to you.

When an entry is returned, it will include a specific reason as to why it was not able to be processed. Based on the return reason indicated, your company will know what its next steps are—correcting the payment and resending it, or handling the issue directly with your client.

[see RETURN on page 2](#)

RETURN continued from page 1

There are many reasons why a transaction may be returned. Two reasons a payment, credit or debit, may be returned are because the recipient's financial institution is unable to locate his/her account or the entry contains an invalid account number. Up until this summer there were these two reasons. These reasons are known as administrative returns and are communicated using return reason codes R03 and R04, respectively. In response to these return reasons, your company can easily determine if you mistyped the account number or whether updated account number information is needed from the recipient before resending the payment.

Typically, entries returned R03 and R04 are nothing to be overly concerned about, as the message conveyed is a simple account number error that is easily correctable. However,

unfortunately, these two return reason codes can also include entries that are fraudulent. These return reason codes didn't send a strong enough message to companies who fell victim to a "pay your bills" scam a few years ago. The scam was publicized on social media and spoke of a special account set up at birth for each of us; ironically, our account number was our Social Security number. This account number coupled with a valid financial institution routing number, which was included in the scam, could be used by consumers when authorizing bill payments.

The impact of the scam was significant to the financial institution whose routing number was provided. Thousands of transactions were initiated daily and rejected due to invalid account numbers. While R03 and R04 were valid reasons to return these payments, these return reasons didn't

differentiate "questionable or suspicious" transactions from routine account number errors (e.g., account number off by a digit, transposition or check serial number added to the account number). Therefore, effective June 21, 2019, return reason code R17 was expanded to send a stronger message to call special attention for a closer review by your company and financial institution.

If you receive an R17 return that includes QUESTIONABLE in the addenda information, know it is being returned for more than an account number error, and it's possible your company may be a victim of fraud. Therefore, it is recommended you perform additional research to ensure your systems are operating properly and have not been compromised. And, if it does turn out to be fraud, contact your financial institution for guidance. 🟢

Securing Data at Your Company

by Jennifer Kline, AAP, APRP, NCP,
Director, Audit Services

It's imperative to the security of the ACH Network that data is secure, and that responsibility falls to financial institutions and businesses alike. These entities are required to establish, implement and update, as appropriate, policies, procedures and systems with respect to protected information. Additionally, all ACH participants must always employ commercially reasonable levels of security from the point of data entry through its transmission. (Reference *ACH Rules*, Sections 1.6 *Security Requirement* and 1.7 *Secure Transmission of ACH Information via Unsecure Electronic Network*).

While the ACH Network and financial institutions rely heavily on the security of banking information and transmission methods, other ACH business users should also employ security methods as part of their



everyday business practices. The Federal Trade Commission provides these tips and advice on the Protecting Small Businesses website to keep sensitive data secure:

1. **Start with security** – Don't collect personal information you don't need. Only hold on to information if you have a legitimate business need.

Don't use personal information when it's not necessary.

2. **Control access to data sensibly** – Restrict access to sensitive data to only appropriate employees and limit administrative access.
3. **Require secure passwords and authentication** – Insist on complex and unique passwords. Store password securely, not on a post-it note beside the computer for everyone to see.
4. **Store sensitive, personal information securely and protect it during transmission** – Keep sensitive information secure throughout its lifecycle, from creation to initiation, to transmission, to storage and finally its destruction.
5. **Segment your network and monitor who's trying to get in and out** – Use firewalls, segment your network and monitor activity on your network.
6. **Secure remote access to your network**
[see DATA on page 4](#)

Mitigating Check Fraud at Your Business

by Marcy Cauthon, AAP, APRP, NCP,
Director, On-Demand Education

Checks are one of the oldest forms of payment in the U.S. and check fraud remains one of the biggest challenges facing businesses today. Using computer technology, criminals find it easy to manipulate checks to defraud consumers and businesses.

Check fraud schemes take many forms. Checks may be:

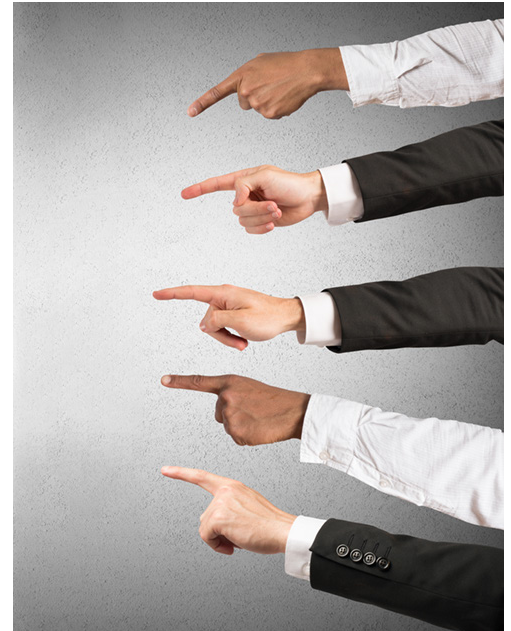
- Altered, either as to the payee or the amount.
- Counterfeited.
- Forged, either as to signature or endorsement.
- Drawn on closed accounts.

Criminals may be insiders, independent operators or part of an organized gang. The methods they use to gain information to commit check fraud include:

- Getting client information from an insider of your company.
- Stealing bank statements and checks.
- Working with dishonest employees of merchants who accept payments by check.
- Rifling through trash for information about bank relationships.

Several warning signs may indicate a bad check. While one sign on its own doesn't guarantee a check to be counterfeit, the greater the number of signs, the greater the possibility that the check is bad. Some common warning signs include:

- A check that doesn't have a MICR (Magnetic Ink Character Recognition) line. These are the numbers and
- A check that has a low sequence number (this could indicate a new account) or a high dollar amount.



- symbols at the bottom of check, printed in magnetic ink that provide information about the name and address of the drawee bank, account number and check number.
- MICR ink that looks shiny or feels raised. Magnetic ink is dull and legitimate check printing produces flat characters.
- A check on which the name and address of the drawee bank are typed rather than printed or includes spelling errors.
- A personal check that has no perforated edge.
- A check showing indications of information that has been altered or erased.

- A signature that appears irregular (shaky or shows gaps in odd spots).
- A check printed on poor quality paper that feels slippery.
- Check colors that smear when rubbed. This suggests they were prepared on a color copier.
- Checks presented at busy times by belligerent or distracting, fast-talking clients.
- Checks that have dollar amounts in numbers and words that don't match.

To mitigate check fraud, businesses need to consider both their internal and external procedures.

[see FRAUD on page 5](#)

· 2019 ·
NACHA
Operating Rules & Guidelines

The Guide to the Rules Governing the ACH Network

Order Your 2019 ACH Rules Today!

Now featuring an app version and online-version
with increased search functionality!


Ensure compliance by making sure you are using the most current Rules available.

DATA continued from page 2

- Ensure endpoint security and put sensible access limits in place.
- 7. **Apply sound security practices when developing new products** – Follow platform guidelines for security, verify that privacy and security features work and test for common vulnerabilities.
- 8. **Ensure your service providers implement commercially reasonable security measures** – Put it in writing, as the security standards should be part of the contract, and verify the service provider's compliance.
- 9. **Put procedures in place to keep your security current and address vulnerabilities that may arise** – Update and patch third-party software, heed credible security warnings and move quickly to fix them,
- 10. **Secure paper, physical media and devices** – Securely store sensitive files, protect devices that process personal information, keep safety standards

in place when data is en route and dispose of sensitive data securely.

More information on Data Security can be found at www.ftc.gov/tips-advice/business-center/small-businesses.

EPCOR encourages all businesses to engage in secure data practices to mitigate any potential risks. 

Ho-Ho-How to Reduce Card Fraud this Holiday Season

by Karen Nearing, AAP, APRP, CAMS, CRCM, NCP, Director, Compliance Education

The holiday season is fast approaching. The online shopping craze will be here before we know it! In many cases, consumers are choosing to use either a debit or credit card to pay for purchases. Your business has an opportunity to lower the number of fraudulent online card transactions processed. Here is how you can help:

1. **Confirm cardholder information.** Ask for the full name, address, phone number and email address. If the billing address differs from the shipping address, follow up with a phone call or email to confirm the order. If you can't reach your customer, don't proceed with the transaction.
2. **Verify the card information. Collect the account number, expiration date and card security code.** Submit the security code with your transaction authorization and evaluate the response. Do not settle transactions for which you received a negative response to your security code inquiry.

3. **Use MasterCard SecureCode and Verified by Visa.** You should support these card authentication services and encourage clients to sign up for them from your website, if they



haven't already done so. MasterCard SecureCode and Verified by Visa protect e-commerce merchants from "cardholder unauthorized" or "cardholder not recognized" types of chargebacks.

4. **Authorize every transaction.** Every e-commerce transaction must be authorized. There are no exceptions, even for recurring transactions, where you had already verified the information.
5. **Don't use voice authorizations.** If you cannot obtain an electronic authorization, try later. Avoid using voice authorizations, as they bypass your processor's system and cannot be used in chargeback re-presentments.
6. **Don't force authorizations.** If your electronic authorization request was declined, request an alternative payment method. Don't call your processor for a voice authorization and force the transaction in your next batch. The processor can still decline the payment. Not to mention, you won't be protected from chargebacks.
7. **Use the Address Verification Service (AVS).** Request an Address Verification Service (AVS) confirmation for all your transactions. AVS compares the billing address provided by your client to the one on file with the card issuer. Don't

see **HOLIDAY** on page 7

FRAUD continued from page 3

Internal Procedure Recommendations

- Review bank statements regularly to detect irregularities.
- Make sure the authorized signers for your business checks are not the same people who reconcile your bank account.
- Know your employees.
- Make sure two people are responsible for accounts payable.
- Ensure mailroom personnel and procedures are sound.
- Keep all check stock or cash equivalents in a secure, locked facility.
- Change keys or entry codes


periodically to prevent routine access to storage areas.

- Consider surprise audits.
- Consider moving check disbursement activity to electronic payment.

External Procedure Recommendations

- Stay current with fraud occurrences in your area and keep a record of when, what and how fraud may hurt your business so you can prevent it the next time.
- Use financial services like positive pay, expedited return information and signature verification systems to protect your accounts payables and accounts receivables.

- Purchase check stock from well-established vendors. If you process your account payables through a service bureau, make sure you have a copy of their security procedures.
- Reconcile your check disbursements and deposits regularly.
- If a payment account is fraudulently used, close the account as soon as possible.
- Find ways to replace paper documents with electronic payment devices.

Resource: <https://www.amfam.com/resources/articles/loss-control-resources/preventing-check-fraud-at-your-business> 

OFAC Compliance Facts Every Business Should Know

OFAC is the acronym for the [Office of Foreign Asset Control](#). OFAC compliance is critical for U.S. businesses working with overseas partners. These regulations are in place in part to ensure that companies don't unwittingly do business with [terrorist organizations](#) or other unsanctioned entities.

The increasing possibility that U.S. businesses, no matter how small, will have foreign suppliers or clients, makes it imperative that they understand the role of Office of Foreign

Asset Control Compliance. Businesses are responsible for following OFAC regulations designed to halt terrorist and other illegal funds from circulating.

If you are in an industry with significant foreign business, a small business owner or an individual doing business, here are the top five areas to familiarize yourself with.

What OFAC Compliance Means

The Office of Foreign Assets Control administers and enforces [economic sanctions](#)

[programs](#) primarily against countries and groups of individuals, such as terrorists and narcotics traffickers. The sanctions can be either comprehensive or selective, using the blocking of assets and trade restrictions to

accomplish foreign policy and national security goals. All U.S. persons (which by legal definition includes firms) must abide by these sanctions—this is the meaning of compliance.



Who Must Be in Compliance?

All U.S. persons must comply with OFAC

regulations, including all U.S. citizens and permanent resident aliens, regardless of where they are located, all persons and entities within the United States, all U.S. incorporated entities and their foreign branches. In the cases of certain programs, such as those regarding Cuba and North Korea, all foreign subsidiaries owned or controlled by U.S. companies also must comply. Certain programs also require foreign persons in possession of U.S. origin goods to comply.

Industry-Specific Information

OFAC provides downloadable guidelines and FAQs for specific industries, including:

- Financial Sector
- Money Service Businesses
- Insurance Industry
- Exporters and Importers
- Tourism / Travel
- Credit Reporting
- Non-Governmental Organizations (NGOs) / Non-profit
- Corporate Registration

OFAC Country and List-Based Sanctions

OFAC Country Sanctions and List-Based Sanctions, including general licenses for exceptions; related documents; and laws, rules and regulations authorizing the sanctions are available on the OFAC Sanctions webpage.

Included in the Country Sanctions List Are:

- The Balkans
- Belarus
- Burma
- Cote d'Ivoire (Ivory Coast)
- Cuba

see OFAC on page 8



There are HUGE Changes Coming in the Payments Industry!

- Regulation CC changes to Funds Availability
- Regulation E Subpart B
- Fraud Threats & Considerations
- Nacha Updates
- FedNowSM

Find out what you need to know to prepare for 2020 and beyond at EPCOR's one-day *Payment Systems Update* seminar.

Registration is opening soon! Watch News You Can Use for details.

Alexa, Can You Read This Article on Voice Assistants?

by Brian Laverdure, AAP, Director,
Emerging Payments Education

Amazon's Alexa now boasts approximately 80,000 "skills," or basically all the actions Alexa can initiate upon voice command from a user. The skills range in complexity, from pulling up random podcasts to updated airport security line wait times, to finding the wind chill or heat index outside. A skill results from a programmer using the Amazon platform to create a customized action(s) based off a set of intents, or what the programmer envisions a person doing with the skill, such as checking a balance. Next, the programmer must identify a series of utterances, the words people will say to activate a skill, combined with an invocation name, which is what people need to say to tie the action to a specific cloud-based service. That sounds easy enough... right?

If you think of any sort of basic statement like, "Alexa, get my balance from ABCD Bank," a person must utter "get my balance from ABCD Bank" for the action to occur. This utterance is specifically tied to ABCD Bank, and APIs will pull the information from ABCD Bank to share with the user. Since Alexa, and other similar voice assistants, rely on the internet to function, all the actions facilitated by the smart speakers or other devices must be able to access an internet-based program. This limitation inhibits voice assistants from offline activities, at least for right now. Think about how much information exists on the internet and you'll realize there is an almost limitless world of

possibilities for voice assistants in any number of industries, including payments.

What comes next for payments and voice assistants? By some estimates, there will be over one-billion voice-assisted devices by 2025, so there will surely be some role to play for this technology in payments and other financial services. As more countries around the world, like Japan, see rapid aging of their populations, these devices are expected to provide enhanced access to people who may suffer from age-related physical conditions that limit their ability to go to a local branch to talk about their accounts. Payments are already a critical component for devices like Amazon's smart speakers, because the Amazon Pay functionality, which supports one-time and recurring payments, is a foundational element in many smart device skills. This makes sense because Amazon, like many of their partners, wants to monetize smart devices and make everyday commerce as simple as possible.

More immediately, however, there are more efforts underway to understand how voice-initiated payments fit into the current payments landscape, rules and regulations. Nacha's Payments Innovation Alliance recently launched a new workgroup

focused on voice-initiated payments, to serve as a forum to identify and debate common challenges regarding voice-initiated payments faced by participants across the payments ecosystem.

Stay tuned to this publication for more educational opportunities. 🌱



EXPLORE EPCOR MEMBERSHIP

EPCOR has membership opportunities for companies, businesses, corporations and Third-Parties.

Explore your options, call 800.500.0100 or email memserve@epcor.org.

HOLIDAY continued from page 4

process the transaction if there is a mismatch.

8. Ship no later than seven days after obtaining an authorization approval.

Ship purchased items as soon as possible. If seven days have passed since obtaining authorization, request a new authorization before shipping.

9. Process authorized transactions within three days of shipping. Do not deposit transactions before shipping

the item, or more than three days after that. Remember that in card-not-present transactions, the shipping date is the transaction date. Don't deposit transactions later than 30 days after the shipping date. If such a transaction is charged back to you, you would not have any recourse.

10. Use the authorization ID for transaction deposits and refunds. The transaction ID returned to you with the authorization approval should be

used with your refunds and deposits. By doing so, you will be able to easily identify fraudulent refund requests, which would lack authorization IDs.

This is not an all-encompassing list, but if you implement these ten procedures in all of your transactions, you will significantly minimize both fraud and chargebacks. We can all work together this holiday season and beyond to make processing card transactions safer for everyone. 🟢

Busting Payments Myths

Myth 1: If Friday is Payday, you won't get your money until Monday

Fact: Payday payments made by Direct Deposit are available in the employees' account at the opening of business on payday in virtually all cases. 93% of American workers use Direct Deposit, enabling faster access to their pay. Workers that get paid via paper checks don't get access to their funds until after their check is cashed or deposited.

Myth 2: Direct Deposits for American Workers are Costly

Fact: Banks, credit unions and employers do not charge employees to receive Direct Deposit to a bank account. Direct Deposits also can help employees avoid fees because money is in their accounts at the opening of business on payday to cover other payments, such as bills.

Myth 3: A Paycheck is a Direct Deposit

Fact: A paycheck is a physical, paper check and is processed through the check collection system. A Direct Deposit is an electronic transfer that is processed through the ACH Network. A paper paycheck is not processed through the ACH Network (even if it is deposited electronically via remote deposit) and cannot be processed on existing or future instant payment systems.

Myth 4: The ACH Network Keeps Bankers' Hours

Fact: The modern ACH Network is open for processing payments 23¼ hours every business day. Files can be submitted to an ACH Operator through 2:15 a.m. ET for settlement at 8:30 a.m. ET.

The ACH Network can only settle payments on business days when the Federal Reserve's settlement service is open.

Myth 5: ACH payments take 3-5 days to process

Fact: The modern ACH Network offers the choice to process all ACH debits as either "same-day" or "next-day" payments. Employers choose to schedule payroll Direct Deposits one to two days in advance. Currently, these processing times do not include weekends and holidays as the Federal Reserve's settlement system is not open.

Myth 6: The U.S. Payments Infrastructure Hasn't been Upgraded in 40 Years

Fact: The modern ACH Network has been continually advanced since its inception. A new Same Day ACH capability went live in 2016. Extended Same Day ACH operating hours are scheduled for March 2021, pending final decision from the Federal Reserve. 🟢

Federal Reserve to Launch FedNowSM

by Brian Laverdure, AAP, Director,
Emerging Payments Education

On August 5, Dr. Lael Brainard, member of the Federal Reserve Board of Governors, announced the Federal Reserve Banks' intent to develop a new, real-time payment system. The system, termed FedNowSM, will bring faster payments to financial institutions of all sizes across the country, and will lay the foundation for the next generation of payments.

The Federal Reserve recognized the need for faster payments years ago when it organized a collaborative a group charged with evaluating how the United States could implement safe and ubiquitous faster payments. In the group's final report issued in 2017, it recommended for the Federal Reserve to create a 24x7x365 settlement service to support real-time payments.

The Federal Reserve moved swiftly to act on the recommendations with a 2018 Federal Register notice, asking for feedback on two possible services to support faster payments. However, the Federal Reserve also clearly stated in the notice that it considered an Real-
see FEDNOW on page 9

For more info on payments myths visit Nacha's newly created webpage at <https://www.nacha.org/content/payments-myth-busting>

Source: Nacha

OFAC continued from page 5

- The Democratic Republic of the Congo
- Iran
- Iraq
- Liberia
- North Korea
- Sudan
- Syria
- Zimbabwe

List-Based Sanctions Programs Include:

- Anti-Terrorism
- Counter Narcotics Trafficking
- Non-proliferation
- Diamond Trading

Specially Designated Nationals (SDN) List

OFAC publishes a [list of Specially Designated Nationals and Blocked Persons](#) (“SDN list”) which includes over 3,500 names of companies and individuals connected with the sanctions targets. A number of the named individuals and entities are known to move from country to country and may end up in unexpected locations. U.S. persons are prohibited from dealing with SDNs wherever they are located and all SDN assets are blocked. It is important to check OFAC’s website on a regular basis to ensure that your SDN list is current. 🌐

Source: ThoughtCo.com

Why it Pays for Nonprofits to Encourage ACH/EFT Donations

It’s a nonprofit no-brainer: Encourage recurring donations through ACH/Electronic funds transfer (EFT).

“Those organizations that have been doing this, that started with EFT early on, they get it,” said Erica Waasdorp, founder and president of the fundraising consulting firm

her organization’s sustainers give via direct debit. Waasdorp said with this nonprofit, there’s a simple explanation: “Because they’ve always had that [ACH/EFT] option on their donation forms and on their platforms.”

In fact, a [Nacha case study](#) of Capital Public Radio in Sacramento, California,



A Direct Solution, and author of *Monthly Giving. The Sleeping Giant*. She works with organizations of all sizes but focuses on small donors—generally \$250 or less—with an emphasis on monthly giving.

At a recent fundraising conference, Waasdorp’s co-presenter told her that 18% of

found that 76% of its sustaining donors pay with ACH, and are responsible for 44% of all individual donation dollars. They also have an 18% greater likelihood of continuing to give after the first 12 months than sustainers who use credit or debit cards.

[see DONATIONS on page 9](#)



Could You Use Some Expert Payments Advice?

If you are considering accepting a new payments type, need a little help creating payments policies or procedures or have any other payments project in the works, EPCOR Advisory Services can help.

Visit epcor.org to find out more about Advisory Services and request a no-obligation quote!



Are You a Third-Party Sender?

If so, don’t forget your ACH Rules Compliance Audit must be completed by **December 31st!**

EPCOR’s *Third-Party Sender ACH Audit Workbook* will walk you through the process.

Or, if you would like an outside set of eyes, contact AmyD@epcor.org to schedule a professional audit with EPCOR.

DONATIONS continued from page 8

So, why isn't every nonprofit embracing direct debits via ACH? Waasdorp answered that question with another question.

"What do they have in place to manage their donations? Many online platforms have added EFT, but not all. There are still many platforms that don't have that option," said Waasdorp, adding it can be especially hard for smaller organizations to get started with ACH/EFT. She explained, "They're busy. They don't really have time."

But it doesn't have to be arduous, and certainly not impossible. Waasdorp has found inexpensive, easy to use platforms with ACH/EFT built in, and nonprofits are starting to embrace them.

Brad Smith, Nacha Senior Director, Industry Verticals said, "nonprofits

shouldn't hesitate to ask their payment providers to make ACH/EFT an option. There are too many positives to accepting donations by ACH/EFT to simply write it off as being 'not available.'"

Waasdorp also noted that "even if your current platform doesn't allow for ACH/EFT yet, one easy way to get started can be by adding a downloadable form with the ACH/EFT option to the website."


You'll find such a form—and a whole lot more—in [Nacha's Nonprofit Toolkit](#), which has everything necessary to start an ACH/EFT donation program or enhance an existing one.

"Among the wealth of items in the Toolkit is information on what's required for ACH authorization, as well as messaging for donors, to dispel some of the myths and

misunderstandings," said Smith. "There are also white papers, case studies and more. Nacha is always ready to help."

For donors who reflexively write a check or give a credit card, Waasdorp said some education might be in order.

"I really think it's a cultural thing," said Waasdorp, who was raised in the Netherlands, where direct debits have been commonplace for decades. "Americans don't necessarily think about the EFT option yet, but as more nonprofits are leading with it, that's starting to change."

Nacha's Nonprofit Toolkit can help your organization get started with ACH or grow your existing program. You'll find the toolkit at [ElectronicPayments.org](#). 


Source: Nacha

FEDNOW continued from page 7

time gross settlement (RTGS) service as the best foundation for the future, and expressed doubts about the private sector's ability to achieve ubiquitous faster payments.

The Federal Reserve provided a description of the service and its potential details in the Federal Register notice that accompanied Governor Brainard's speech:

- Individual payments processed within seconds, 24 hours a day, 7 days a week, 365 days a year
- Service will only support credit transfers—there will be no debit functionality
- It will support a wide variety of use cases, including P2P transfers, bill payment and B2B payments
- Interbank settlement will occur in real-time through credit/debit entries to master accounts at Reserve Banks (or possibly a correspondent bank)
- Service will launch with individual payments limited to \$25,000 or less

Although much about FedNowSM currently remains uncertain, the Federal Reserve anticipates introducing the system in 2023 or 2024. Stay tuned for more information. 

White Paper Examines the Effects of Synthetic Identity Payments Fraud

Synthetic identity payments fraud is a fast-growing but little-understood problem that affects individuals, financial institutions, government agencies and private industry. The severity of this type of fraud is documented in a [white paper](#) released by the Federal Reserve System.

A [synthetic identity](#) is created by using a combination of real information (such as a legitimate Social Security number) with fictional information (which can include a made-up name, address or birthdate). Fraudsters use synthetic identities to commit payments fraud, which can escape detection by today's identity verification and credit-screening processes. Over time, fraudsters build up the synthetic identity's creditworthiness, then purchase high-value goods and services on credit and disappear. Because the identity was not real to begin with, there is limited recourse in tracing the perpetrators and holding them responsible. Consumers whose identities have been used for fraud face the

time-consuming process of correcting their credit reports. Other consequences extend beyond payments fraud to include denial of disability benefits, rejection of tax returns and inaccuracies in health records.

"Crime rings see attractive opportunities in synthetic identity payments fraud," said Ken Montgomery, Federal Reserve System payments security strategy leader and chief operating officer at the Federal Reserve Bank of Boston. "Law enforcement officials, financial institutions and other organizations recognize it as a growing concern. But unfortunately, many consumers don't realize how it can hurt their access to credit or how to protect themselves," he said. "The white paper provides information on the current state of synthetic identity fraud, including the scope of the issue, causes, contributing factors and its impact on the payments industry."

Visit [FedPaymentsImprovement.org](#) to learn more.

Source: FederalReserve.gov



PEOPLES
NATIONAL BANK



Electronic Payments Core of Knowledge

EPCOR is a not-for-profit payments association which provides payments expertise through education, advice and member representation. EPCOR assists banks, credit unions, thrifts and affiliated organizations in maintaining compliance, reducing risk and enhancing the overall operational efficiency of the payment systems. Through our affiliation with industry partners and other associations, EPCOR fosters and promotes improvement of the payments systems which are in the best interest of our members. For more information on EPCOR, visit www.epcor.org.



Nacha[™]
Direct Member

EPCOR, as a Direct Member of NACHA, is a specially recognized and licensed provider of ACH education, publications and support.

© 2019, EPCOR. All rights reserved.

www.epcor.org

3100 Broadway Blvd., Ste. 555, Kansas City, MO 64111

800.500.0100 | 816.474.5630 | fax: 816.471.7665